TUGAS MID

Keamanan Jaringan Komputer

DISUSUN OLEH

NAMA : AVID JONRA

NIM : 09121001048

SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

INDRALAYA

2016

`1. Scaning

-NMAP

```
20/tcp    open  tcpwrapped
21/tcp    open  ftp         Pure-FTPd
22/tcp    open  ssh         OpenSSH 5.3 (protocol 2.0)
24/tcp    open  tcpwrapped
25/tcp    open  tcpwrapped
32/tcp    open  tcpwrapped
37/tcp    open  tcpwrapped
42/tcp    open  tcpwrapped
53/tcp    open  domain?
79/tcp    open  tcpwrapped
80/tcp    open  http        nginx 1.9.12
81/tcp    open  tcpwrapped
82/tcp    open  tcpwrapped
84/tcp    open  tcpwrapped
85/tcp    open  tcpwrapped
88/tcp    open  tcpwrapped
90/tcp    open  tcpwrapped
106/tcp   open  tcpwrapped
109/tcp   open  tcpwrapped
110/tcp   open  pop3        qmail pop3d
111/tcp   open  rpcbind     2-4 (RPC #100000)
119/tcp   open  tcpwrapped
143/tcp   open  imap        Courier Imapd (released 2005)
```

Open Port

-NESSUS

Host Information

DNS Name:	itera.ac.id
IP:	180.250.46.219

Results Summary

Critical	High	Medium	Low	Info	Total
0	1	8	4	227	240

Tingkat Vulnerability

-NETCUT

```
avid@avid:~$ nc -v -w 3 -z itera.ac.id 80
DNS fwd/rev mismatch: itera.ac.id != 219.subnet180-250-46.speedy.telkom.net.id
itera.ac.id [180.250.46.219] 80 (http) open
avid@avid:~$ nc -v -w 3 -z itera.ac.id 21
DNS fwd/rev mismatch: itera.ac.id != 219.subnet180-250-46.speedy.telkom.net.id
itera.ac.id [180.250.46.219] 21 (ftp) open
avid@avid:~$ nc -v -w 3 -z itera.ac.id 22
DNS fwd/rev mismatch: itera.ac.id != 219.subnet180-250-46.speedy.telkom.net.id
itera.ac.id [180.250.46.219] 22 (ssh) open
avid@avid:~$ nc -v -w 3 -z itera.ac.id 110
DNS fwd/rev mismatch: itera.ac.id != 219.subnet180-250-46.speedy.telkom.net.id
itera.ac.id [180.250.46.219] 110 (pop3) open
avid@avid:~$
```

Open Port & Service

2. Analisa

2.1 Open Port

-Port 21

Port 21 pada server itera.ac.id terbuka, ini memberikan informasi bahwa server itera.ac.id memiliki laayanan FTP (File Transfer Protokol)

-Port 80

Port 80 pada server itera.ac.id terbuka, ini memberikan informasi bahwa port ini menggunakan protokol http sebagai media komunikasi dengan user dan memiliki layanan web server.

-Port 22

Port 22 pada server itera.ac.id terbuka, ini memberikan informasi bahwa port ini memiliki layanan remote server melalui protokol SSH (Secure Shell)

2.2 Daemon

-Pure FTPd

Software ini merupakan aplikasi FTP yang mengizinkan user untuk upload dan download file. Sistem ini hanya menampilkan file yang memang dimiliki oleh user.

-Open SSH 5.3 (Protocol 2.0)

Dengan protokolSSH user dapat mengirimkan file dan melakukan remote server jarak jauh dengan trafic yang terenkripsi sehingga memberikan keamanan data yang di kirim oleh user

-Nginx 1.9.12

Nginx merupakan salah satu software atau daemon untuk membangun web server seperti apache

2.3 Vulnerability

-Pure FTPd

Pada port 21 ini tidak dapat diketahui tidak versi dari software yang digunakan pada server, tetapi dari informasi CVE menemukan kelemahan pada software ini yaitu rentan terhadap serangan directory traversal yaitu bug dimana user dapat mengakses directory lain yang bukan merupakan directory yang menjadi layanan dari sistem.

-Open SSH 5.3 (Protocol 2.0)

Server ini menggunakan versi SSH dari software Open SSH 5.3, dari informasi yang didapatkan dari CVE versi ini memiliki kelemahan yang disebabkan oleh bug heap-based Buffer Overflow yang dapat mengakibatkan software mengalami crash sehingga layanan remote tidak berjalan. Ini merupakan bug yang terjadi karena memori tidak mampu menampung data khususnya string yang melebihi kapasitas memori.

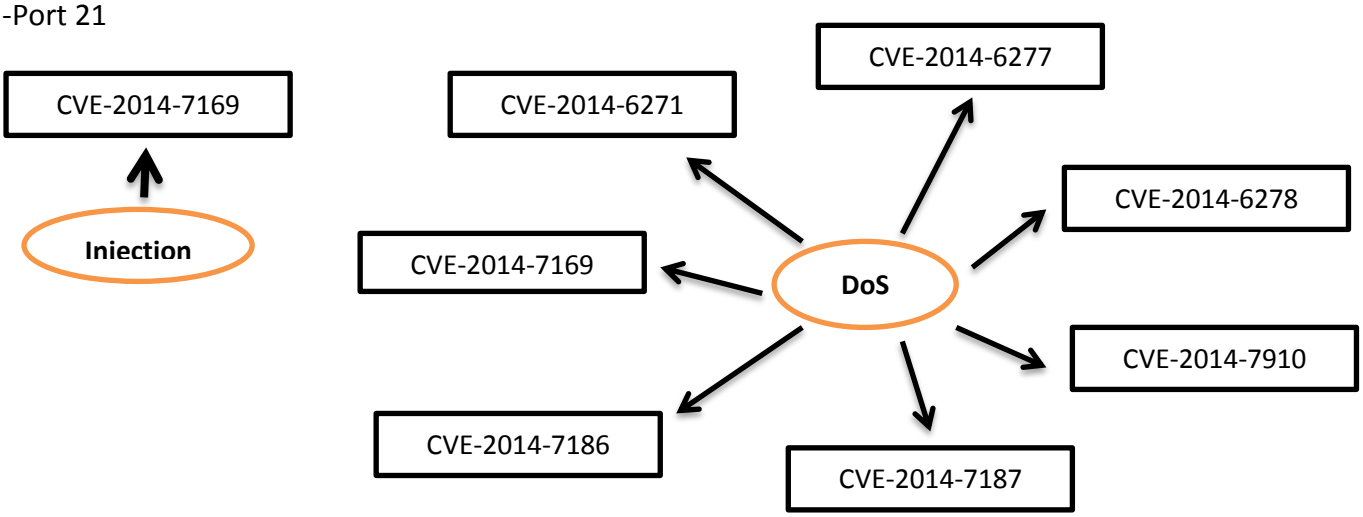
-Nginx 1.9.12

Software Nginx pada versi ini dari informasi yang didapatkan dari CVE belum menemukan kelemahan , kelemahan baru terdapat pada Nginx versi sebelum 1.9.10. dan juga belum menemukan keterkaitan CVE.

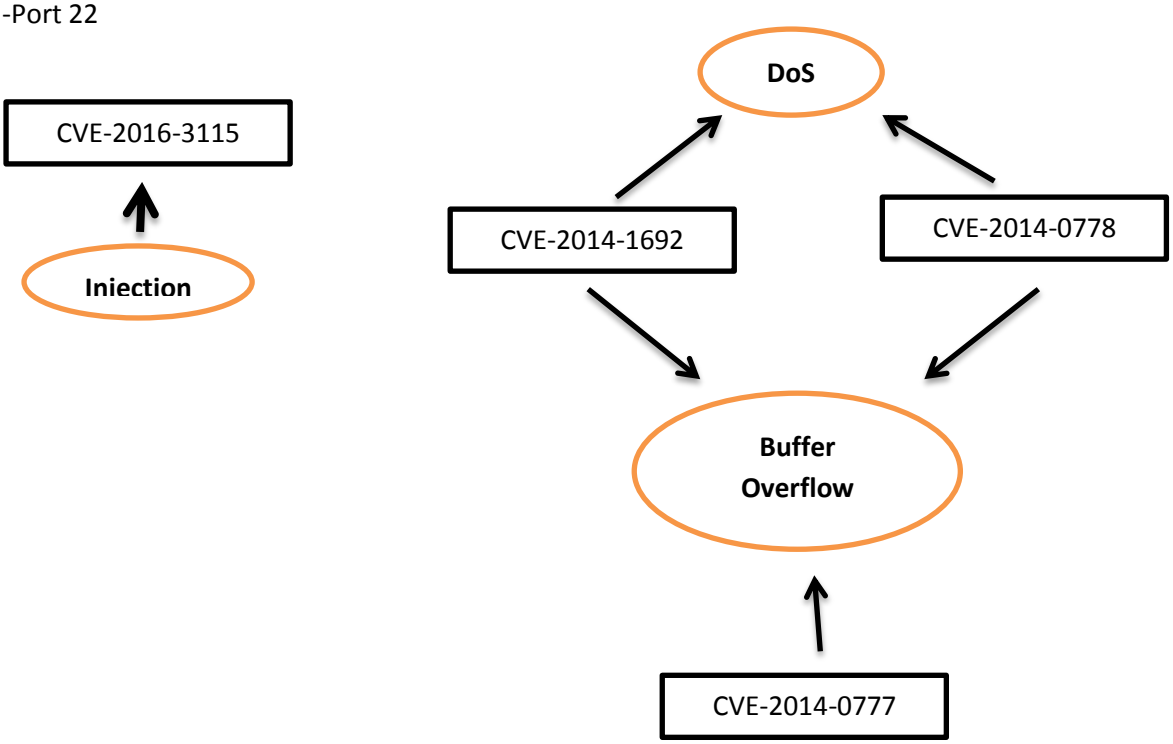
3. CVE

Map CVE

-Port 21



-Port 22



-Port 80

Dari informasi CVE, server itera.ac.id menggunakan Nginx versi 1.9.12 dan belum ditemukan Vulnerability pada versi ini . Vulnerability baru terdapat pada versi sebelumnya.